

ABSTRACT OF THE DISCLOSURE

Systems and methods for monitoring a network. Proxy loghosts, each one collecting log files that are generated by resources in a portion of a secure network, generate events in response to the log files collected. A central loghost in communication with the proxy loghosts receives the events from the proxy loghosts, analyzes the events, and determines the necessity of generating an alert and an associated alarm to notify a security manager of a possible intrusion incident, or other anomaly, in the network.

Document #: 1251026 v.1